JOURNAL LA EDUSCI

VOL. 03, ISSUE 02 (058-068), 2022
DOI: 10.37899/journallaedusci.v3i2.633

Little Fermat Theorem Applying for Problems about Division

Nguyen Tuyet Nga[1]

[1]*Tan Trao University, Tuyen Quang, Vietnam*

**Corresponding Author: Nguyen Tuyet Nga*
Email: tuyetngasp@gmail.com

Article Info

Article history:
Received 3 March 2022
Received in revised form 27 March 2022
Accepted 31 March 2022

Keywords:
Divisibility
Prime
Positive Integer
Remainder

Abstract

This article provides solutions to some divisibility problems using Fermat's little theorem. To have beautiful solutions for each of those problems, mathematicians have combined knowledge of: Theory of divisibility and division with remainder, greatest common divisor, least common multiple, prime numbers, congruences, exponentiation, etc. This helps students think positively and flexibly about their existing knowledge and skills, and present concise and creative solutions.

Introduction

Solving an arithmetic problem using theorems has always been an attraction for every mathematician (Singh, 2017; Ostrowski, 2016). In particular, arithmetic is one of the basic content in the high school math program and is featured in national and international competitions for excellent students and many other math competitions (Ellison & Swanson, 2010; Hyde & Mertz, 2009). Fermat's little theorem is one of the most famous and useful theorems in mathematics, which is applied in many different fields (Hilbert, 1902). The study of Fermat's little theorem, in addition to providing mathematical knowledge, also helps students to analyze, research, explore, exploit, develop problems to generalize, generalize knowledge and improve high thinking about problem solving. In addition, in-depth study of this theorem is also an effective tool to solve intensive problems of congruence, perfect squares, co-prime numbers, paired primes, etc., which are frequent topics (Stein, 2008). present on Math forums, Math meetings, Student Math Olympiads, as well as related fields (Lehrer & Chazan, 2012).

Methods

Authors use experiences, observations and examples with explanatory method to illustrate results and draw conclusion. Author also use dialectical materialism methods.

Results and Discussion

Some Knowledge to Remember

[1, p. 502] Fermat's Little Theorem: If p is a prime and a is a positive integer then $a^p \equiv a \pmod{p}$

Prove 1.

Use induction by a.

With a = 1 tense, the proposition is always true.

Assume that the statement is true a I.e $p \mid a^p - a$

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

We will prove the statement to be true $a+1$. *Indeed:*

$$(a+1)^p-(a+1)=(a^p-a)+\sum_{i=1}^{p-1}C_p^k a^k$$

Using $p\,|\,C_n^k,\ (1\le k\le p-1)$ *and assuming induction we deduce.* $p\,|\,(a+1)^p-(a+1)$. *Then* $(a+1)^p\equiv(a+1)\ (\text{mod }p)$

So we complete the proof.

Prove 2.

Assume that $(a,\ p)=1$ *and it is necessary to prove that* $a^{p-1}\equiv1\,(\text{mod }p)$

Consider integers $a,2a,...,(p-1)a$ *whose remainders when divided by p distinct (otherwise, with* $ia\equiv ja\,(\text{mod }p)$ then $p\,|\,(i-j)a$ or $p\,|\,i-j$, sign"=" happens if $i=j$).

So $a,2a,...,(p-1)a\equiv1.2....(p-1)\ (\text{mod }p)$

It mean $a^{p-1}(p-1)!\equiv(p-1)!\ (\text{mod }p)$

So $(p,(p-1)!)=1$ *we infer what we have to prove.*

Note. This theorem can be abbreviated as: $a^{p-1}\equiv1\,(\text{mod }p)$

[2, p. 27] Definition of Divisibility

An integer a is said to be divisible by an integer $b\ (b\neq0)$ if there exists an integer x such that $a=bx$. Then we say that a is multiple of b or b is a divisor of a and denoted by $a\,\vdots\,b$ or $b\,|\,a$. If a is not divisible by b, we denote it $a\,\not\vdots\,b$ or $b\nmid a$, then we write $a=bq+r$ and call $r=0,1,2,r-1$ the remainder in division a cho b.

[3, p. 3] Properties of Divisibility

+) If $a\,\vdots\,b$ then $ac\,\vdots\,b$ with $\forall c\in Z$

+) If $a\,\vdots\,b$ and $b\,\vdots\,c$ then $a\,\vdots\,c$

+) If $a\,\vdots\,c$ and $b\,\vdots\,c$ then $(ax+by)\,\vdots\,c$ with all integer $x,\ y$

+) If $a\,\vdots\,b$ and $a,\ b>0$ then $a\ge b$

+) If $a\,\vdots\,b$ and $b\,\vdots\,a$ then $a=b$ or $a=-b$

+) If $m\neq0$ and $a\,\vdots\,b$ then $a=b\Leftrightarrow am\,\vdots\,bm$

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

Some Practical Exercise

Exercise 1: *Prove that* $m=\dfrac{9^{47}-1}{8}$ *an odd composite number is not divisible by 3 and* $3^{m-1}\equiv 1 \pmod{m}$

The answer:

First, we show that m *the composite number is odd. Indeed:*

We have $m=\dfrac{9^{47}-1}{8}=\dfrac{3^{47}-1}{2}.\dfrac{3^{47}+1}{4}$

Since $\dfrac{3^{47}-1}{2},\dfrac{3^{47}+1}{4}$ *are all integers greater than 1, m is composite*

Comment $m=\dfrac{9^{47}-1}{8}=\dfrac{9^{47}-1}{9-1}=9^{46}+9^{45}+...+9+1\equiv 1 \pmod{3}$, I.e m not divisible by 3

Comment: 9^{k} *ends in 9 if k is odd and ends in 1 if k is even*

So $9^{46}+9^{45}\,9^{46}+9^{45}+...+9^{2}+9=(9^{46}+9^{45})+(9^{44}+9^{43})+...+(9^{2}+9)$

Obviously, each sum in brackets ends with the digit 0, and 46 is even, so the sum above consists of 23 pairs. Thus, m ends with the digit 1, so m is odd

Now we will prove $3^{m-1}\equiv 1 \pmod{m}$

According to Fermat's little theorem, then $9^{47}\equiv 9 \pmod{47}$

As $9^{47}\equiv 9 \pmod{8}$ and $(47,8)=1$ then $9^{47}\equiv 9 \pmod{47.8}$

It means that $m-1=\dfrac{9^{47}-9}{8}\,\vdots\,47$

As 46 I seven number and $(2;46)=1$ then $(m-1)\,\vdots\,94$

From that $(3^{m}-1)\,\vdots\,(2^{94}-1)\Rightarrow(3^{m}-1)\,\vdots\,m$ (do $(3^{2p}-1)\,\vdots\,8m$

Or $3^{m-1}\equiv 1 \pmod{m}$

Exercise 2: With $p=5$ is prime and a,b are two odd natural numbers such that $a+b\,\vdots\,5$ and $a-b\,\vdots\,4$. Prove $a^{b}+b^{a}\,\vdots\,10$

Tee answer:

Assume $a\geq b$

Call r is the remainder in division a by 5 then $a\equiv r \pmod{5}$ (1) (do $a+b\,\vdots\,5$)

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

From
$a\equiv r \pmod 5 \Rightarrow a+b\equiv r+b \pmod 5 \Rightarrow b+r\equiv 0 \pmod 5 \Rightarrow b\equiv -r \pmod 5$

$a\equiv r \pmod 5 \Rightarrow a^b \equiv r^b \pmod 5$

$b\equiv -r \pmod 5 \Rightarrow b^a \equiv (-r)^a \pmod 5$

At that time $a^b+b^a\equiv r^b - r^a \pmod 5 \Rightarrow a^b+b^a \equiv r^b(1-r^{a-b}) \pmod 5$

On the other hand, by assumption $a-b \vdots 4$ then $a-b \vdots 4.k$

As r is not divisible by 5, so by Fermat's little theorem, we have:

$a^b+b^a\equiv r^4 \equiv 1 \pmod 5 \Rightarrow r^{4.k}\equiv 1 \pmod 5 \Rightarrow r^{a-b}\equiv 1 \pmod 5$

From that we get: $a^b+b^a\equiv 0 \pmod 5$, I.e $a^b+b^a \vdots 5$

Furthermore: a^b, b^a are odd integers, so $a^b+b^a \vdots 2$

Hence: $a^b+b^a \vdots 10$

Exercise 3: Prove with $\forall k=1,\ 2,\ 3,...,\ 100$ then $C_{101}^k \vdots 101$

The answer:

Put $f(x)=\sum_{k=1}^{100} C_{101}^k x^k = (x+1)^{101}-(x^{101}+1)$ with $\forall x\in \mathbb{Z}$

Apply theorem little Fermat we have:

$(x+1)^{101}\equiv x+1 \pmod{101}, \forall x\in \mathbb{Z}$

On the other hand, according to theorem Fermat, we have: $x^{101}\equiv x \pmod{101}$, from that $x^{101}+1\equiv x+1 \pmod{101}$, $\forall x \in \mathbb{Z}$

This leads to equation $f(x)=0 \pmod{101}$ has 101 solutions.

As $\deg\ f = 100$ then f not have level $\bmod 101$, i.e all coefficients of f divisible by 101. We have what to be proved.

Exercise 4: Prove with $\forall k=1,\ 2,\ 3,...,\ 36$ then $C_{36}^k \equiv (-1) \pmod{37}$

The answer:

Consider polynomial

$$f(x)=(x+1)^{36}-\frac{x^{37}+1}{x+1}$$

Comment: f mod's 37 rank is not over 35 or it has no rank

Apply theorem little Fermat we see equation $f(x)\equiv 0 \pmod{37}$ has 36 solutions mod 37 are $0, 1,..., 35$. This means that all coefficients of f are divisible by 37

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

Hence $C_{36}^{k} \equiv (-1)(\text{mod } 37), 1 \leq k \leq 36$

Exercise 5: Prove with $\forall a,b \in Z$ then $(ab^7 - ba^7) \vdots 7$

The answer:

We have $ab^7 - ba^7 = ab(b^6 - a^6)$. Then:

+) If $7 | ab$ then $7 | ab(b^6 - a^6) = ab^7 - ba^7$

+) If $7 \nmid ab$ then as $(7, a) = 1, (7, b) = 1$ according to theorem little Fermat we have $b^7 \equiv b \ (\text{mod } 7) \Rightarrow b^6 \equiv 1 \ (\text{mod } 7)$ (1)

Also, according to theorem little Fermat, we have $a^7 \equiv a \ (\text{mod } 7) \Rightarrow a^6 \equiv 1 \ (\text{mod } 7)$ (2)

From (1) and (2) $\Rightarrow b^6 - a^6 \equiv 0 \ (\text{mod } 7)$

Or $7 | b^6 - a^6 \Rightarrow 7 | ab^7 - ba^7$

Thus, with $\forall a,b \in Z$ then $(ab^7 - ba^7) \vdots 7$

Exercise 6: Prove $37^{40} + 41^{36} - 1 \vdots 37.41$

The answer:

As 41 a prime, apply theorem little Fermat we have $37^{41} \equiv 37 \ (\text{mod } 41)$.

From that $37^{41} - 37 \equiv 0 (\text{mod } 41) \Rightarrow 37(37^{40} - 1) \equiv 0 (\text{mod } 41)$ (1)

As $(37, 41) = 1$ so from (1) we have: $37^{40} - 1 \equiv 0 (\text{mod } 41)$ (2)

Obviously $41^{36} \equiv 30 (\text{mod } 41)$ (3)

From $(2), (3)$ we have $37^{40} + 41^{36} - 1 \equiv 0 \ (\text{mod } 41)$

Because roles of $41, 37$ the same we have: $41^{36} + 37^{40} - 1 \equiv 0 \ (\text{mod } 37)$

As $(37, 41) = 1$ then $41^{36} + 37^{40} - 1 \equiv 0 \ (\text{mod } 41.37)$

From that $37^{40} + 41^{36} - 1 \vdots 37.41$ (what to be proved)

Exercise 7: Prove $(3^{97} - 2^{97} - 1) \vdots 42.97$

The answer:

As 97 a prime according to theorem little Fermat we have:

$3^{97} \equiv 3 (\text{mod } 97), \ 2^{97} \equiv 2 (\text{mod } 97)$

So:

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

$$3^{97} - 2^{97} \equiv 1 (\text{mod } 97) \Rightarrow 3^{97} - 2^{97} - 1 \equiv 0 (\text{mod } 97)$$
$$\Leftrightarrow (3^{97} - 3) - (2^{97} - 2) \equiv 0 (\text{mod } 97)$$
$$\Leftrightarrow 3^{97} - 2^{97} - 1 \equiv 0 (\text{mod } 97)$$
$$\Leftrightarrow (3^{97} - 2^{97} - 1) \vdots\, 97 \ (*)$$

On the other hand: $3^{97} - 2^{97} - 1 = [(3^{97} - 1) - 2^{97}] \vdots\, 2$ (1)

Then $3^{97} - 2^{97} - 1 \equiv -(-1)^{97} - 1 \equiv 0 \ (\text{mod } 3)$, I.e $3^{97} - 2^{97} - 1 \vdots\, 3$ (2)

Now we prove $(3^{97} + 2^{97} - 1) \vdots\, 17$

We have:

$$3^{97} - 2^{97} - 1 = 3.3^{96} - 2^{97} - 1$$
$$= 3.3^{2.48} - 2^{97} - 1$$
$$= 3.(3^2)^{48} - 2^{97} - 1$$
$$= 3.9^{48} - 2^{97} - 1$$
$$\equiv 3.2^{48} - 2^{97} - 1 \ (\text{mod } 7)$$

And $3.2^{48} - 2^{97} - 1 = (2+1).2^{48} - 2^{97} - 1 = 2^{49} + 2^{48} - 2^{97} - 1$

So:

$$3^{97} - 2^{97} - 1 \equiv 2^{49} + 2^{48} - 2^{97} - 1 \ (\text{mod } 7)$$
$$\equiv 2^{49} + (2^3)^{16} - 2^{97} - 1 \ (\text{mod } 7)$$
$$\equiv 2^{49} + 8^{16} - 2^{97} - 1 \ (\text{mod } 7)$$
$$\equiv (8^{16} - 1) + 2^{49} - 2^{97} \ (\text{mod } 7)$$
$$\equiv 2^{49} - 2^{97} \ (\text{mod } 7)$$
$$\equiv -(2^{97} - 2^{49}) \ (\text{mod } 7)$$
$$\equiv -(2^{49}(2^{48} - 1)) \ (\text{mod } 7)$$
$$\equiv -(2^{49}(8^{16} - 1) \ (\text{mod } 7)$$
$$\equiv 0 \ (\text{mod } 7) \ (3)$$

From (1), (2), (3) we have $(3^{97} - 2^{97} - 1) \vdots\, 42$ (**)

From (*) and ((**) we have: $(3^{97} - 2^{97} - 1) \vdots\, 42.97$

Exercise 8: Find all positive integers n such that $2^n - 1 \vdots\, 7$

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

The answer:

As 2 a prime according to theorem little Fermat, we have $2^7 \equiv 2 \pmod 7$

From that $2^6 \equiv 1 \pmod 7 \Rightarrow 2^6 - 1 \equiv 0 \pmod 7$, and $2^6 - 1 = (2^3 - 1)(2^3 + 1)$, so $7 \mid (2^3 - 1)(2^3 + 1) \Rightarrow 7 \mid 2^3 + 1 \Leftrightarrow 2^3 \equiv 1 \pmod 7$

So all numbers n divisible by 3 satisfying requirement.

Exercise 9: Prove that there are infinitely many positive integers n that satisfy $(2^n - 1) \vdots 67$

The answer:

As 2 a prime according to theorem little Fermat, we have $2^{67} \equiv 2 \pmod{67}$

From that $2^{66} \equiv 1 \pmod{67} \Rightarrow 2^{m.66} \equiv 1 \pmod{67}$, with m positive integer.

Take $n = m.66$, with $m \equiv -1 \pmod{67}$, we have $n = m.66 \equiv 1 \pmod{67}$

And $2^n - n \equiv 2^n - 1 \equiv 0 \pmod{67}$

So, there are infinitely many positive integers m such that $m \equiv -1 \pmod{67}$ there are infinitely many positive integers n satisfying $(2^n - 1) \vdots 67$

Exercise 10: [5, tr. 45] Prove $3^{100} - 3 \vdots 13$

The answer:

As 13 a prime, according to theorem Fermat we have:

$3^{12} \equiv 1 \pmod{13}$

With $100 = 12.8 + 4$ so $3^{100} = (3^{12})^8.3^4 \equiv 3^4 \pmod{13}$

But $3^4 \equiv 81 \equiv 3 \pmod{13}$

Then the remainder in division $3^{100} - 3$ by 13 is 0, or $3^{100} - 3 \vdots 13$

Exercise 11: With $n \geq 2, a \geq 0$ is a positive integer and m is a prime such that $a^m \equiv 1 \pmod{m^n}$. Prove if $m > 2$ then $a \equiv 1 \pmod{m^{n-1}}$ and if $m = 2$ then $a \equiv \pm 1 \pmod{2^{n-1}}$

The answer:

We have $a^m \equiv 1 \pmod{m^n}$ with $n \geq 2$, so $a^m \equiv 1 \pmod m$

From theorem little Fermat $a^m \equiv a \pmod m$, so $a \equiv 1 \pmod m$

In case a = 1, Obviously there is something to prove

If $a \neq 1$, we put $a = 1 + km^u$ (here $u \geq 1$ and $k \not\vdots\, m$. So, $m > 2$, $a^m = 1 + km^{u+1} + Vm^{2u+1}$ with V an integer

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

Hence *m + 1 > n* so $a \equiv 1 \pmod{m^{n-1}}$

In case $m = 2$, we have $2^n \mid a^2 - 1 = (a-1)(a+1)$

As $a - 1 \neq 2, a + 1 \neq 2$ so $a - 1, a + 1$ both cannot be multiples of 4. So either expression $a - 1, a + 1$ is divisible by 2^{n+1}, I.e $a \equiv \pm 1 \pmod{2^{n-1}}$. We have what to be proved

Exercise 12: With a as integer, knowing $a^{25} - a \vdots m \ (m > 1)$. Find *m*

The answer:

Suppose to find a number m that satisfies the requirements of the problem. Then with p is a prime number, because p^2 is not divisible by $p^{25} - p$, so we have p^2 not divisible by m. So m multiples of distinct primes

On the other hand, we have: $a^{25} - 2 = 2.3^2.5.7.13.17.241$

As $3^{25} \equiv -3 \pmod{17}$ and $3^{25} \equiv 32 \pmod{241}$ so m not divisible by 17 and 241.

According to theorem little Fermat, we have $a^{25} \equiv a \pmod{p}$ when $p = \{2; 3; 5; 7; 13\}$

Thus, m will be equal to the divisors of: 2. 3. 5. 7. 13, different from 1 and have $2^5 - 1 = 31$ their divisors.

Exercise 13: Let t be a positive integer, k be an odd natural number and $m = k.2^t + 1$an odd prime number. Assume that for x, y are natural numbers satisfying $x^{2^t} + y^{2^t} \vdots m$. Prove that then x, y simultaneously divisible by m.

The answer:

We prove it by the method of contradiction

Assume the opposite, $x \not\vdots\, m$, then $y \not\vdots\, m$

As m a prime according to theorem little Fermat we have: $x^{m-1} \equiv 1 \pmod{m}, y^{m-1} \equiv 1 \pmod{m}$.

As $m - 1 = k.2^t$ then we have: $x^{k.2^t} \equiv 1 \pmod{m}, y^{k.2^t} \equiv 1 \pmod{m}$

From that we get $x^{k.2^t} + y^{k.2^t} \equiv 2 \pmod{m}$. (1)

According to assumption $x^{2^t} + y^{2^t} \vdots m \Leftrightarrow x^{2^t} + y^{2^t} \equiv 0 \pmod{m}$

Because k odd natural number:

$$x^{k.2^t} + y^{k.2^t} = (x^{2^t})^k + (y^{2^t})^k \vdots (x^{2^t} + y^{2^t}) \equiv 0 \pmod{m} \ (2)$$

We see (1) and (2) contradict. So x and y at the same time divisible by m (what to be proved)

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

Exercise 14: Using theorem Fermat find remainder when divide 3456^{789} by 23

The answer:

According to theorem Fermat, we get:

$$3456^{789} \equiv (3456^{789})^{35} . 3456^{19}$$
$$\equiv 1^{35} . 6^{19} \pmod{23}$$
$$\equiv 6^{19} \pmod{23}$$
$$\equiv 6^{18} .6 \pmod{23}$$
$$\equiv 6^{3.6} .6 \pmod{23}$$
$$\equiv (6^3)^6 .6 \pmod{23}$$
$$\equiv 9^6 . 6 \pmod{23}$$
$$\equiv (9^2)^3 .6 \pmod{23}$$
$$\equiv 12^3 . 6 \pmod{23}$$
$$\equiv 3 . 6 \pmod{23}$$
$$\equiv 18 \pmod{23}$$

So remainder when divide 3456^{789} by 23 is 18

Exercise 15: Prove $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \vdots 7$

The answer:

The numbers 1; 2; 3; 4; 5; 6 is a co-prime to 7, so by Fermat's theorem we have the following congruences:

$$1^6 \equiv 1 \pmod{7};$$
$$2^6 \equiv 1 \pmod{7};$$
$$3^6 \equiv 1 \pmod{7};$$
……………………….
$$6^6 \equiv 1 \pmod{7};$$

Raising to the third power on both sides of the above congruence, we get: $1^{18} \equiv 1 \pmod{7}$

$$2^{18} \equiv 1 \pmod{7}$$
$$3^{18} \equiv 1 \pmod{7}$$
……………………….

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

$6^{18} \equiv 1 \pmod 7$

Adding the sides of those congruent, we get:

$$1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv 0 \pmod 7$$

$$\Leftrightarrow 1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \vdots 7$$

Exercise 16: With m is prime and $m > 5$. Prove $m^8 - 1 \vdots 240$

The answer:

Analyze 240 Product analysis of prime factors (standard form), we get $240 = 2^4.3.5$

Apply little Fermat theorem, we have $m^4 \equiv 1 \pmod 5$ and $m^2 \equiv 1 \pmod 3$

Call a positive integer, we see $(a,\ 2^4) = 1$ when a is odd.

On the other hand apply formula $\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})....(1 - \frac{1}{p_k})$ is the number of smaller than m and prime positive numbers with m (với $m = p_1^{m_1}.p_2^{m_2}....p_k^{m_k}$ is the standard analysis of m), we get $\varphi(24) = \varphi(2^3.3) = 24.(1 - \frac{1}{2}).(1 - \frac{1}{3}) = 8 = 2^3$

According to theorem Euler, we get $m^8 \equiv 1 \pmod{16}$.

Hence $m^8 \equiv 1 \pmod p$ with $p = 3, 5, 16$. From that $m^8 - 1 \vdots 240$ (what to be proved)

Exercise 17: With p as a prime and $p - 2 \vdots 3$. Prove with a, b are integers satisfying $a^3 - b^3 \vdots p$ then $a - b \vdots p$

The answer:

Consider 2 cases: a or b divisible by p and a, b are not divisible by p

+) Case 1: If $a \vdots p \Rightarrow b^3 \vdots p \Rightarrow b \vdots p$, so $a - b \vdots p$

+) Case 2: If a, b are not divisible by p

As assumption $p - 2 \vdots 3 \Rightarrow p = 3k + 2\ (k \in \mathbb{N})$

According to little Fermat theorem, we get $a^{p-1} \equiv 1 \pmod p$

But $p = 3k + 2\ (k \in \mathbb{N})$ then $a^{3k+1} \equiv 1 \pmod p$

Similar proof, we get $b^{3k+1} \equiv 1 \pmod p$

From that $a^{3k+1} - b^{3k+1} \vdots p$

According to assumption $a^3 - b^3 \vdots p \Rightarrow a^{3k} - b^{3k} \vdots p$

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)

From that $a-b \vdots p$ (what to be proved).

Conclusion

The diverse and complex topics of Arithmetic problems are always attractive to good students, because solving each problem in this field helps train and develop students' thinking. Using Fermat's little theorem to solve divisibility problems, in addition to providing quick, concise and accurate solutions, also stimulates new discoveries and discoveries in problem solving, helping learners to be creative in learning. Through this type of math, learners have the ability to think deeply, the ability to flexibly apply knowledge content to each type of exercise accordingly, so that they can achieve the best effect to meet the program. new general education with the goal of orienting student capacity development.

Acknowledgement

This research is funded by Tan Trao University in Tuyen Quang, Viet Nam.

References

Ellison, G., & Swanson, A. (2010). The gender gap in secondary school mathematics at high achievement levels: Evidence from the American Mathematics Competitions. *Journal of Economic Perspectives*, *24*(2), 109-28.

Hilbert, D. (1902). Mathematical problems. *Bulletin of the American Mathematical Society*, *8*(10), 437-479.

Hyde, J. S., & Mertz, J. E. (2009). Gender, culture, and mathematics performance. *Proceedings of the National Academy of Sciences*, *106*(22), 8801-8807.

Lehrer, R., & Chazan, D. (2012). Teachers and Students Investigating and Communicating About Geometry: The Math Forum. In *Designing Learning Environments for Developing Understanding of Geometry and Space* (pp. 479-502). Routledge.

Ostrowski, A. M. (2016). *Solution of Equations and Systems of Equations: Pure and Applied Mathematics: A Series of Monographs and Textbooks, Vol. 9* (Vol. 9). Elsevier.

Singh, S. (2017). *Fermat's enigma: The epic quest to solve the world's greatest mathematical problem*. Anchor.

Stein, W. (2008). *Elementary number theory: primes, congruences, and secrets: a computational approach*. Springer Science & Business Media.

ISSN 2721-0979 (Print), ISSN 2721-1258 (Online)